Network Analyzer

DR. Sarang M. Patil[1], Ganesh S. Gudewar[2], Dhananjay N. Korde[3], Rushikesh Ingale[4], Shivam Koli[5]

[1] HOD , [2 3 4 5] BE Students , Department of Computer Engineering SKNSITS, Lonavala, India.

hodce.sknsits@sinhgad.edu , ganeshgudewar.sknsits.comp@gmail.com

Abstract : In the ever-expanding realm of modern technology, the stability and efficiency of communication networks have become vital to our daily lives, the continuity of businesses, and the functioning of entire industries. To meet the growing demands of network management and optimization, the Network Analyzer Project emerges as a pioneering endeavor. This project envisions the development of a comprehensive system tailored to empower network professionals and administrators in their mission to monitor, analyze, and enhance network performance. The Network Analyzer Project is committed to the creation of that components include data collection and log capture mechanisms, robust data storage and management systems, visualization tools, real-time network monitoring capabilities, and an array of troubleshooting and diagnostic utilities.

Keywords : ***IP Blocking, Network Analyzer, Network Troubleshooting, Packet Sniffing, Port Scanning .***

I. INTRODUCTION

In an ever-evolving technological landscape, this project stands at the nexus of innovation, with its core objectives encompassing both hardware and software components. These include cutting-edge data collection, storage and management systems, real-time network monitoring, and an array of diagnostic utilities.

In addition to its monitoring and analysis capabilities, the Network Analyzer Project offers insight into the active network system. Users can access vital information such as system name, version, and active ports, ensuring a comprehensive view of the network's current state.

The Network Analyzer Project represents a pivotal step in the evolution of network management, aiming to enhance network reliability, security, and performance. As we embark on this journey, we anticipate a future where network administrators possess the tools they need to ensure the seamless operation of our interconnected world.

II. OBJECTIVES

Create an intuitive user interface for Network Monitoring and Analysis, featuring a user-friendly dashboard with interactive visuals, customizable widgets, and easy navigation. The interface provides a quick overview of network performance, logs, and security alerts while allowing in-depth data analysis.

Establish real-time network monitoring with continuous data collection, processing, and dynamic reporting, including historical trend analysis for long-term network optimization.

Strengthen network security analysis by integrating an IP blocklist feature to proactively identify and list malicious IP addresses that could threaten system integrity and data security.

Provide essential diagnostic tools for network administrators and engineers, including a traceroute for network mapping and a ping utility for the device reachability checks.

Improve data management by enabling seamless export of network log data in CSV and TXT formats for analysis and reporting, along with support for data import to facilitate historical analysis.

III. LITERATURE SURVEY

The internet has become an integral part of modern society, transforming social processes. Its widespread adoption has brought a surge in internet users, but also a concerning rise in cyber security threats [1].

The development of application software and technology changes gradually. In order to meet the customers' specific requirements and ensure the robustness and efficiency of the application software, various functions are packaged as a whole[2].

The situation is further compounded by the rapid development of mobile internet, cloud computing, and Network Function Virtualization (NFV) technologies. These advancements, while creating a complex IT infrastructure, create a larger attack surface for potential security breaches [3].

This increasingly complex environment fosters new security risks. The likelihood and impact of security incidents like intrusion attacks, web tampering, and DDoS attacks are all on the rise. Additionally, the emergence of novel threats necessitates the development of more robust security solutions and improved risk management strategies[4].

Network Analyzer Tool provides the ideal blend of conceptual instruction and work to give administrators and

 DOI : 10.35291/2454-9150.2024.0159

users a quick start in monitoring network systems using the operating system[5].

Network and information security are paramount for safeguarding individual privacy and community well-being. Attackers are constantly innovating, employing sophisticated tools and techniques to breach security measures [6]. Traditional firewall technology alone is no longer sufficient to protect critical systems, necessitating a layered approach to network defense [7].

The evolving cyber landscape demands continuous upgrades and vulnerability patching of defense equipment, placing a significant burden on network administrators. Even minor negligence can have severe consequences, highlighting the need for robust security solutions [8].

Intrusion Detection Systems (IDS), when paired with appropriate network analysis tools, can effectively identify and mitigate security threats, ensuring network uptime and data integrity [9].

As a result, High-End Network Analyzer systems have become a focal point of research due to their crucial role in securing networks across diverse environments. Packet niffing is a process that is used to intercept and log traffic passing over a network. We can use JPcap and Winpcap to capture these packets from the network. We use the Python network packet capture method to collect all packets [10].

IV. SYSTEM OVERVIEW AND DESIGN

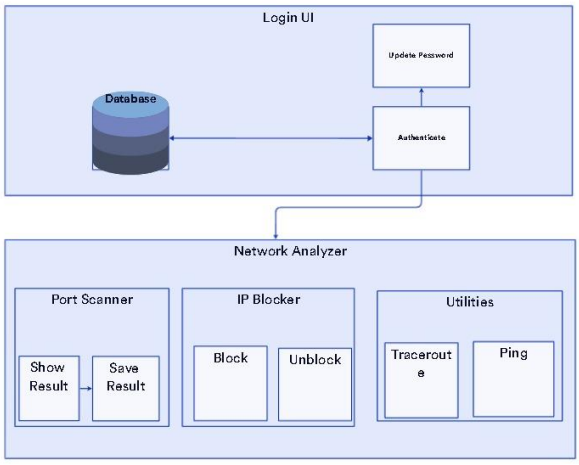

Figure 1 : Architecture Diagram

The system architecture outlined here illustrates a two-module network management tool. The first module focuses on secure user access. It utilizes a login system with predefined usernames and passwords for authentication. Additionally, it allows users to update their passwords, promoting security best practices.

The second module provides a comprehensive toolkit designed for network analysis and troubleshooting. This toolbox includes a network analyzer to identify potential network issues, a port scanner to assess vulnerabilities by identifying open ports on devices, an IP blocker to manage network access by restricting specific IP addresses, and ping & traceroute utilities to verify network connectivity and diagnose network path problems.

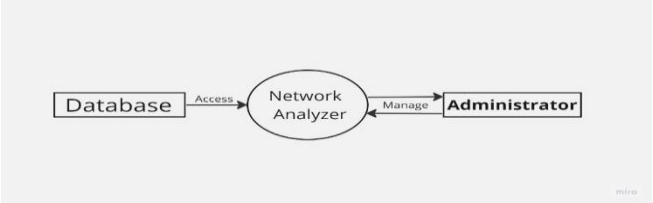

Figure 2 : DFD LEVEL 0

This simple diagram outlines the core concept of the network analyzer system. It depicts a single box representing the entire system, where network administrators input commands and network data. The system then processes this information and provides results like reports and visualizations back to the administrators, essentially acting as a black box for network analysis.

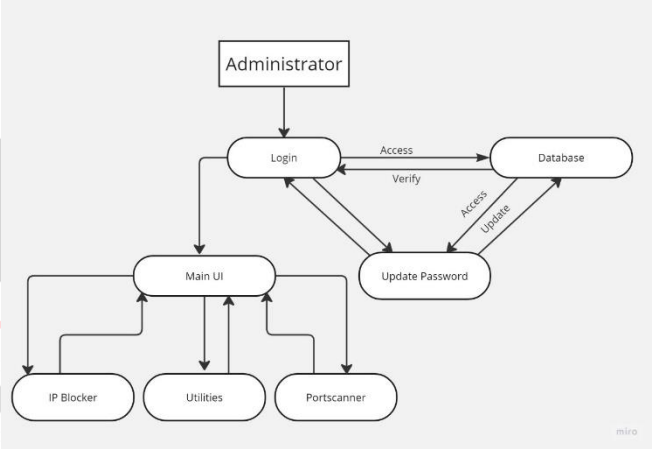

Figure 3 : DFD LEVEL 1

This DFD Level 1 dives deeper than the basic blueprint, showing how the network analyzer system works internally. It expands the single "Network Analyzer" process into four steps: receiving user input, gathering network data, analyzing that data, and finally generating reports or visualizations for the administrator. Data flows between these steps and the external user, illustrating how information moves through the system for network analysis.

V. METHODOLOGY

1. USER AUTHENTICATION AND AUTHORIZATION SYSTEM:

Developed and implemented a tailored user authentication and authorization system as part of our network monitoring and analysis tool. Despite having a single-user account setup, the system was designed to verify the user's identity securely before granting access to the monitoring tool, effectively safeguarding against unauthorized network access.

This approach focused on enhancing security by enforcing stringent controls over access privileges and permissions. The implementation of this system played a critical role in ensuring secure and controlled access to the network monitoring functionalities within our project.

 DOI : 10.35291/2454-9150.2024.0159

2. INTERFACE SELECTION AND DATA COLLECTION:

In our study, we undertook a deliberate approach to select appropriate network interfaces for data capture within our network monitoring and analysis tool. We carefully evaluated and opted for either Wi-Fi or Ethernet network cards based on specific requirements and considerations. Additionally, we integrated sophisticated filtering capabilities, allowing us to focus data capture efforts on specific ports, IP addresses, or protocols of interest.

This tailored approach ensured comprehensive yet efficient data collection, facilitating accurate analysis and real-time monitoring of network activities. By leveraging these selected interfaces and filtering techniques, we achieved enhanced network visibility and improved performance management, aligning with the objectives of our research project.

3. DATA PROCESSING AND ANALYSIS:

Concentrated on the precise processing and analysis of collected network data as part of network monitoring and analysis.

Our methodology focused on efficiently preprocessing raw network packets to extract essential metadata, including source/destination IP addresses, protocols, packet length, and timestamps.

By emphasizing rigorous data processing techniques, our research highlights the importance of foundational analysis for improving network visibility and operational efficiency in network monitoring systems. This approach lays the groundwork for effective network management and performance optimization based on comprehensive data analysis.

4. USER INTERFACE :

The interface was designed to present real-time monitoring data, diagnostic tools, and network analytics in a user-friendly manner. Emphasis was placed on simplicity and clarity to ensure ease of navigation and clear presentation of critical information to users.

Through this interface, users could access and interpret real-time network performance metrics, utilize diagnostic tools for troubleshooting purposes, and leverage network analytics for deeper insights into network activities.

This user-centric design approach aimed to enhance usability, facilitate efficient network monitoring, and contribute to overall user productivity within the network management domain. The intuitive interface design was pivotal in supporting effective network operations management within our research framework.

5. TROUBLESHOOTING TOOLS :

The troubleshooting tools module within our project comprises a suite of utilities designed to aid network engineers and IT professionals in diagnosing and resolving network issues efficiently. This module includes tools such as network topology mapping, packet capture analysis, protocol analyzers, and ping/traceroute utilities.

These tools collectively assist in visualizing network architecture, analyzing network logs, and diagnosing connectivity and latency issues. By leveraging these troubleshooting capabilities, users can effectively identify and address network performance issues and connectivity problems, thereby enhancing the overall reliability and efficiency of network operations.

6. EXPORT FUNCTIONALITY:

Implemented comprehensive export and reporting functionalities within our network monitoring and analysis tool. The primary objective was to enable users to export relevant network data and generate detailed reports for further analysis and documentation.

This feature allows users to export network traffic data in standard formats such as PCAP (Packet Capture) for offline analysis and forensic investigation purposes. By enabling the extraction of raw network data, this capability supports in-depth examination and troubleshooting of network issues.

The export functionality serves as a valuable tool for network engineers and analysts, providing access to detailed network traffic data that can be utilized for post-incident analysis.

7. TESTING AND VALIDATION :

In our project, a rigorous testing and validation process was implemented to ensure the functionality, performance, and reliability of each module and the integrated system as a whole.

This comprehensive approach included conducting unit tests to evaluate the individual components of each module and integration testing was performed to assess the interaction and interoperability between different modules within the system, confirming seamless integration of functionalities and data exchange.

Through these iterative testing procedures, we aimed to identify and address any issues early in the development cycle, ensuring the successful implementation and deployment of the network monitoring and analysis system.

 DOI : 10.35291/2454-9150.2024.0159

VI. APPLICATION RESULT

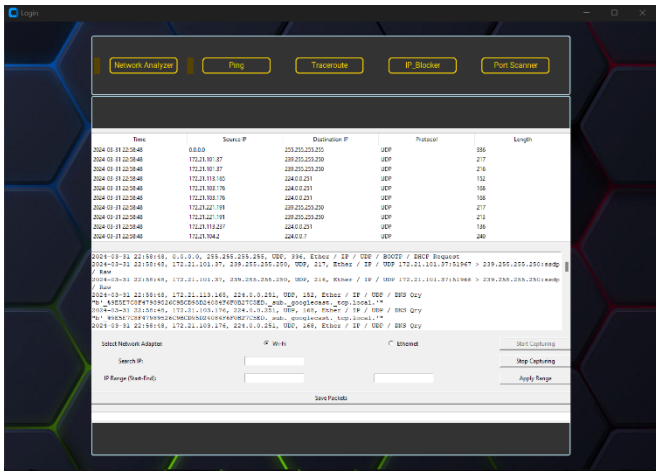

Figure 4 : Network Analyzer

A Network Analyzer typically displays a variety of information about captured network traffic, including details about the traffic itself, the protocols used, packet headers, and timestamps.

Network Analyzer software allows users to select the network adapter or interface through which they want to capture network traffic. users can often search for specific IP addresses within traffic.

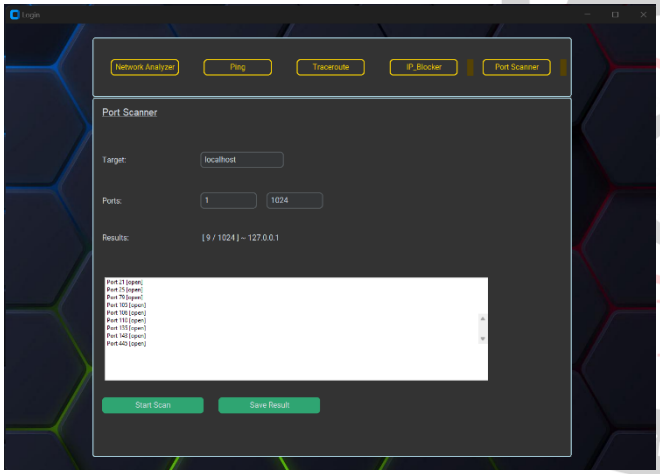

Figure 5 : Port Scanner

A port scanner looks through your whole IP address block for active hosts inside the given IP address range.

These ports serve as communication channels between the host and other network devices. This program then searches ports to see whether services are running on them and to detect open ports.

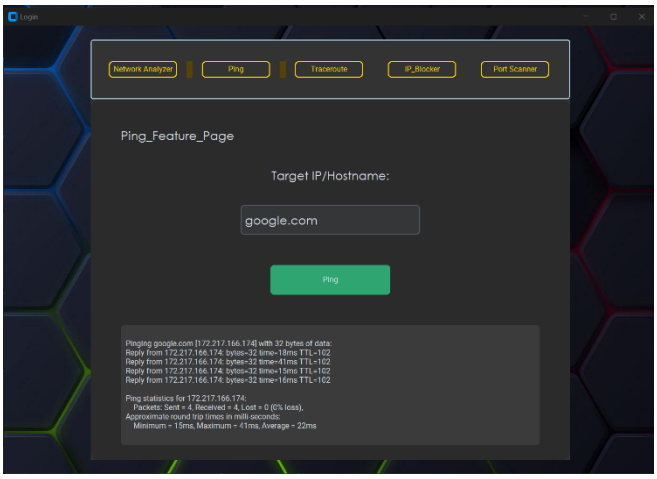

Figure 6 : Ping

Ping is a word used in internet speed test results to determine how quickly a data signal goes from one network device to another. It is critical to determining how long it takes for a packet of data to go from your device to a server and then back to your device.

Ping is an excellent tool for checking network connectivity by delivering data packets and monitoring response time. It is used to diagnose network difficulties by determining whether a device can communicate with another device on the local network or the internet.

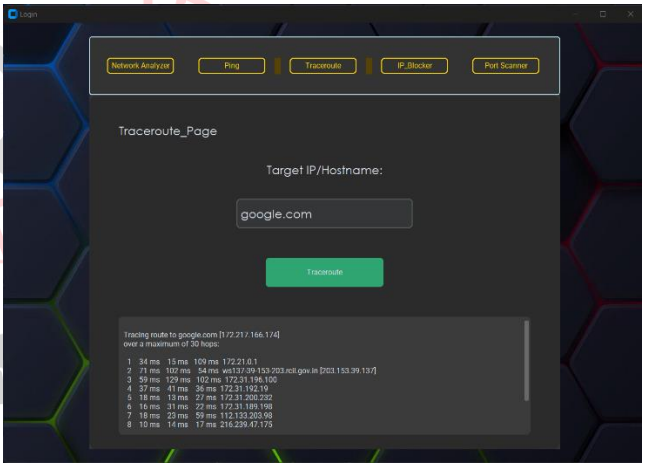

Figure 7 : Traceroute

Get the whole path taken by a packet to reach its destination. Learn the names and identities of the routers and devices in the path. Determine how long it takes to send and receive data from each device in the path.

Traceroute traces the route of your information packets. So, you can see the whole journey that your data packets follow to get to their destination.

The devices (hosts) that were used along the travel of your information packets will also be included in the tracing findings.

 DOI : 10.35291/2454-9150.2024.0159

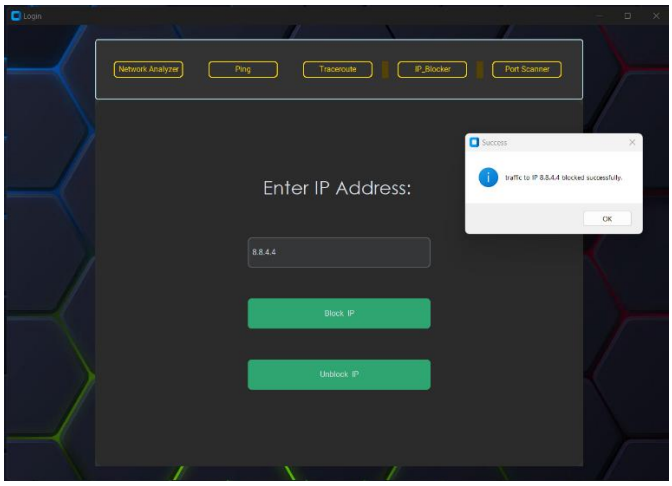

Figure 8 : IP Blocker

An IP blocker feature is designed to prevent specific IP addresses from communicating with or accessing certain resources on a network.

It is a security feature that allows network administrators to control and restrict access to their network based on the source IP addresses of incoming traffic.

VII. CONCLUSION

In conclusion, the Network Analyzer Project presented in this paper represents a significant contribution to the field of network management and optimization. The project addresses the growing demands of modern communication networks by providing a comprehensive system equipped with data collection, monitoring, and diagnostic capabilities.

Through the development of an intuitive user interface and proactive security features such as IP blocking, the Network Analyzer Project aims to enhance network reliability, security, and performance. The integration of essential diagnostic tools like traceroute and ping utilities further empowers network administrators in troubleshooting and optimizing network operations.

The project's emphasis on real-time monitoring, historical trend analysis, and seamless data export capabilities underscores its commitment to providing network professionals with the tools necessary for effective network management. By facilitating efficient data processing and analysis, the Network Analyzer Project contributes to improved network visibility and operational efficiency.

Moving forward, the insights and methodologies presented in this paper lay the groundwork for future advancements in network analysis and management. The project's comprehensive approach and user-centric design exemplify best practices in network monitoring and optimization, paving the way for a more secure and reliable interconnected world.

VIII. FUTURE ENHANCEMENT

In summary, the successful completion of Final Phase paves the way for the subsequent phases of the Network Analyzer Project. With a well-defined roadmap, a motivated team, and a comprehensive understanding of the project's scope, we are well prepared to be advance with new features.

Here, we will initiate further development and testing, bringing us one step closer to delivering a network analysis tool that fulfils the needs of our users.

IX. REFERENCES

[1] M. Fuentes-García, J. Camacho, and G. Maciá-Fernández, "Present and future of network security monitoring," IEEE Access, vol. 9, pp. 112744–112760, 2021.

[2] R. Nazir, K. Kumar, S. David, and A. A. Laghari, "Survey on wireless network security," Archives of Computational Methods in Engineering, vol. 1, pp. 1–20, 2021.

[3] G. Liu, B. Peng, and X. Zhong, "A novel epidemic model for wireless rechargeable sensor network security," Sensors, vol. 21, no. 1, p. 123, 2021.

[4] S. Sengupta, A. Chowdhary, A. Sabur, and D. HuangA. AlshamraniS. Kambhampati, "A survey of moving target defenses for network security," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1909–1941, 2020.

[5] M. Zhao, G. Wei, C. Wei, and Y. Guo, "CPT-TODIM method for bipolar fuzzy multi-attribute group decision making and its application to network security service provider selection," International Journal of Intelligent Systems, vol. 36, no. 5, pp. 1943–1969, 2021.

[6] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," Journal of Network and Computer Applications, vol. 169, Article ID 102767, 2020.

[7] Y. Zhou, T. A. Mazzuchi, and S. Sarkani, "M-adaboost-a based ensemble system for network intrusion detection," Expert Systems with Applications, vol. 162, Article ID 113864, 2020.

[8] J. Pei, K. Zhong, J. Li, J. Xu, and X. Wang, "ECNN: Evaluating a cluster-neural network model for city innovation capability," Neural Computing & Applications, pp. 1–13, 2021, https://doi.org/10.1007/s00521-021-06471-z.

[9] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset," IEEE Access, vol. 8, pp. 29575–29585, 2020.

[10] M. Pawlicki, M. Choraś, and R. Kozik, "Defending network intrusion detection systems against adversarial evasion attacks," Future Generation Computer Systems, vol. 110, pp. 148–154, 2020.

[11] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging

 DOI : 10.35291/2454-9150.2024.0159

Telecommunications Technologies, vol. 32, no. 1, Article ID e4150, 2021.

[12] C. Deng and H. Qiao, "Network security intrusion detection system based on incremental improved convolutional neural network model," in International Conference on Communication and Electronics Systems, pp. 1–5, Coimbatore, India, 21-22 Oct. 2016.

[13] Z. Wu, J. Wang, L. Hu, Z. Zhang, and H. Wu, "A network intrusion detection method based on semantic re-encoding and deep learning," Journal of Network and Computer Applications, vol. 164, Article ID 102688, 2020.

[14] R. Magán-Carrión, D. Urda, I. Díaz-Cano, and B. Dorronsoro, "Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches," Applied Sciences, vol. 10, no. 5, p. 1775, 2020.

[15] W. Elmasry, A. Akbulut, and A. H. Zaim, "Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic," Computer Networks, vol. 168, p. 107042, 2020.

[16] Mrinal Kanti Debbarma "Performance analysis of network monitoring tool through automated software engineering approach", Dept CSE , National Institute of Technology, Agartala, India , 10.1109/SPACES.2015.7058294 IEEE

[17] Zineb Moussaoui "Network Security Traffic Analysis Platform-Designand Validation",19th (AICCSA) , Abu Dhabi, United Arab Emirates,10.1109/AICCSA56895.2022.10017862 , IEEE/ACS 2022.

[18] Abdullahi S.B Mohammed "Network Traffic Analysis: A Case Study of ABU Network" April 2013 University Sains Malaysia , Research Gate:10.5120/2222-2863.

[19] Mostafijur Rahman, Z. Khalib , R. B. Ahmad "Performance Evaluation of PNtMS: A Portable Network Traffic Monitoring System on Embedded Linux Platform" 2009 ICCET Singapore 10.1109/ICCET.2009.37 IEEE.

[20] A. Dabir, A. Matrawy "Bottleneck Analysis of Traffic Monitoring using Wireshark" 2007 10.1109/IIT.2007.4430446

IEEE Xplore / ICIIT.

[21] M. Qadeer, A. Iqbal, Mohammad Zahid, M. Siddiqui Computer Science "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer" 2010 Second (ICCNT),

IEEE Xplore 10.1109/ICCSN.2010.104.

[22] SiewYeen Agnes Tan, I. Jacobs, Yao Liang Computer Science, Engineering "A Network Measurement Tool for Handheld Devices" 2003 IEEE Xplore.

[23] X. Yang, A.P. Petropulu, "The Extended Alternating Fractal Renewal Process for Modeling Traffic in High-Speed Communication Networks," IEEE Trans. Sig. Proc., vol. 49, no. 7, July 2001.

[24] Victor S. Frost and Benjamin Melamed, Traffic Modeling for Telecommunications Networks, IEEE Communications, Mar. 1994.

[25] B.G. Barnett; E.T. Saulnier "High level traffic analysis of a LAN segment" [1992] Proceedings 17th Conference on Local Computer Networks , Minneapolis, MN, USA , 10.1109/LCN.1992.228159 IEEE.

 DOI : 10.35291/2454-9150.2024.0159